EXHIBIT A-2
IDENTIFICATION OF PRIOR ART THAT ANTICIPATES AND/OR RENDERS OBVIOUS THE ASSERTED '661 CLAIMS
PATENT L.R. 3-3(B)

ASSERTED CLAIM	IDENTITY OF PRIOR ART THAT ANTICIPATES AND/OR RENDERS OBVIOUS THE ASSERTED CLAIM
1. A cryptographic processing device for securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret by external monitoring, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) a source of unpredictable information; (c) a processor: (i) connected to said input interface for receiving and cryptographically processing said quantity, (ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by modifying said sequence; and (d) an output interface for outputting said cryptographically processed quantity to a	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Sci.crypt Postings Dunlavy '201 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the above listed references, individually or in combination with one or more of the following references: Ugon '833 Griffin '294 Sci.crypt Postings Dunlavy '201 Hoppe '894 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) ISO 7816

recipient thereof.	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Griffin '294, the Sci.crypt Postings, and Dunlavy '201 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
2. The device of claim 1 wherein said input	**ANTICIPATION**

interface and said output interface are the same element.	The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following reference: Dunlavy '201 The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious by any of the references or combinations of references showing obviousness of claim 1. Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. For example, ISO 7816 shows standard pin assignments, which include an I/O

	interface. Each of Ugon '833 and Dunlavy '201 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, either of these references renders the claim obvious, alone or in combination with any of the above listed references.
4. The device of claim 1 wherein said cryptographic processing operation includes transforming a message with the Data Encryption Standard (DES).	**OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references: Ugon '833 Sci.crypt Postings Griffin '294 Dunlavy '201 individually or in combination with one or more of the following references: Ugon '833 Sci.crypt Postings Griffin '294 Dunlavy '201 Menezes (1997) FIPS PUB 46-2 (1993) Wakerly (1989) Rankl (1997) Hoppe '894 ISO 7816 Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed

	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. For example, FIPS PUB 46-2 (1993) describes the DES standard and suggests its use in certain microprocessors. Additionally, Menezes (1997) at 250 discusses DES as a well-known cryptographic algorithm.
5. A cryptographic processing device for securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret by external monitoring, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) a source of unpredictable information; (c) a processor: (i) connected to said input interface for receiving and cryptographically processing	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Sci.crypt Postings Lindholm '725 Van Eck '117 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references: Sci.crypt Postings Ugon '833 Lindholm '725 Van Eck '117

said quantity, (ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by randomizing the order of said permutation; and (d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.	Dunlavy '201 individually or in combination with one or more of the following references: Sci.crypt Postings Ugon '833 Lindholm '725 Van Eck '117 Dunlavy '201 Hoppe '894 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) ISO 7816 FIPS Pub 46-2 (1993) Menezes (1997) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed

	components had been or could be used with cryptographic processing devices. For example, Menezes (1997) at 10 teaches that permutations are commonly used in cryptographic operations. Each of Lindholm '725, the Sci.crypt Postings, and Van Eck '117 fully anticipates the claim by disclosing all claim elements either explicitly or implicitly or under the doctrine of inherency. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
6. A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) a source of unpredictable information; (c) a processor: (i) connected to said input interface for receiving and cryptographically processing said quantity, (ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity in said microchip during said processing; and (d) an output interface for outputting said	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Fruhauf '053 Griffin '294 Sci.crypt Postings Lisimaque '039 Saltwick '243 Malek '467 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references: Ugon '833 Fruhauf '053 Griffin '294 Sci.crypt Postings Lisimaque '039 Saltwick '243

cryptographically processed quantity to a recipient thereof.	Malek '467 Van Eck '117 Høivik '098 Dunlavy '201 Lindholm '725 Lindholm '713 individually or in combination with one or more of the following references: Ugon '833 Fruhauf '053 Griffin '294 Sci.crypt Postings Lisimaque '039 Saltwick '243 Malek '467 Van Eck '117 Høivik '098 Dunlavy '201 Lindholm '725 Lindholm '713 Guthery (1998) Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Guillou (1986) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed

	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. For example, one of ordinary skill in the art would be motivated to combine Rankl (1997) (describing subscriber networks as a potential implementation of smartcards) with Griffin '294. Further, Guthery teaches that smartcards are frequently designed having single-chip processors. Dunlavy '201 suggests (*e.g.*, at 8:13-19) its implementation on any type of computer, computer peripheral or other type of electronic device. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Fruhauf '053, Griffin '294, the Sci.crypt Postings, Lisimaque '039, Saltwick '243, and Malek '467 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of

	these references renders the claim obvious, alone or in combination with any of the above listed references.
7. The device of claim 6 including program logic to activate said expending during said processing.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Van Eck '117 Griffin '294 Sci.crypt Postings Lisimaque '039 Malek '467 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references: Ugon '833 Dunlavy '201 Van Eck '117 Sci.crypt Postings Griffin '294 Lisimaque '039 Malek '467 alone or in combination with one or more of the following references: Ugon '833 Dunlavy '201 Van Eck '117 Sci.crypt Postings

	Griffin '294 Lisimaque '039 Malek '467 Guthery (1998) ISO 7816 Hoppe '894 Wakerly (1989) Rankl (1997) Guillou (1986) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Each of Ugon '833, Van Eck '117, Griffin '294, the Sci.crypt Postings, Lisimaque '039, and Malek '467 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above

	listed references.
8. The device of claim 7 including (a) program logic implementing said source of unpredictable information; and (b) program logic to transmit said unpredictable information to an additional power expending circuit contained in said microchip.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Lisimaque '039 Malek '467 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references: Ugon '833 Dunlavy '201 Lisimaque '039 Malek '467 individually or in combination with one or more of the following references: Ugon '833 Dunlavy '201 Lisimaque '039 Malek '467 Guthery (1998) Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Guillou (1986)

	Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Each of Ugon '833, Lisimaque '039, and Malek '467 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
9. A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Fruhauf '053 Lindholm '713 Malek '467 Dunlavy '201 Griffin '294

portion of a message; (b) a source of unpredictable information; (c) a processor: (i) connected to said input interface for receiving and cryptographically processing said quantity, (ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity; (d) an output interface for outputting said cryptographically processed quantity to a recipient thereof; (e) a hardware-implemented noise production subunit connected to said source of unpredictable information and configured to expend unpredictable amounts of electricity based on the output of said source of unpredictable information; and (f) an activation controller, which may be activated by software contained in said device, to activate and deactivate said expending of unpredictable amounts of electricity.	The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 Wuidart '917 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Fruhauf '053 Lindholm '713 Malek '467 Dunlavy '201 Griffin '294 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Fruhauf '053 Lindholm '713 Malek '467 Dunlavy '201 Griffin '294 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the

	references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Fruhauf '053, Lindholm '713, Malek '467, Dunlavy '201, Griffin '294 and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
10. The device of claim 9 wherein said	**OBVIOUSNESS**

source of unpredictable information is a hardware-implemented random number generator, and wherein said noise production subunit includes a digital-to-analog converter.	The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Lindholm '713 Malek '467 Dunlavy '201 Griffin '294 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Lindholm '713 Malek '467 Dunlavy '201 Griffin '294 JP10197610 JP10084223 JP62082702 JP62260406 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective

	functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices.
11. A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising: (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; (c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and (d) a noise production system for introducing noise into said measurement of said power consumption.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Sci.crypt Postings Fruhauf '053 Sprunk '402 Lisimaque '039 Kolbert '057 Lindholm '725 Meyr '962 Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833

	Wuidart '917 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Griffin '294 Sci.crypt Postings Fruhauf '053 Sprunk '402 Lisimaque '039 Kolbert '057 Lindholm '725 Meyr '962 Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Griffin '294 Sci.crypt Postings Fruhauf '053 Sprunk '402 Lisimaque '039 Kolbert '057 Lindholm '725

	Meyr '962 Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either

	explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Griffin '294, the Sci.crypt Postings, Fruhauf '053, Sprunk '402, Lisimaque '039, Kolbert '057, Lindholm '725, Meyr '962, Nossen '423, Lindholm '713, Saltwick '243, Malek '467, Van Eck '117, Dunlavy '201, Høivik '098, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
12. The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic; (b) a noise processing module for improving the random characteristic of said initial noise; and (c) a noise production module configured to vary said power consumption based on an output of said noise processing module.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 Wuidart '917 **OBVIOUSNESS**

	The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Griffin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Griffin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed

	above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Each of Ugon '833, Griffin '294, Fruhauf '053, Lindholm '725, Lindholm '713, Saltwick '243, Malek '467, Høivik '098, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
13. The device of claim 12 wherein said noise production system is connected to said processor and is selectively operable under the control of said processor.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Lindholm '713 Malek '467 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 Wuidart '917 **OBVIOUSNESS**

	The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Griffin '294 Fruhauf '053 Lindholm '713 Malek '467 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Griffin '294 Fruhauf '053 Lindholm '713 Malek '467 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the

	references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Each of Ugon '833, Griffin '294, Lindholm '713, Malek '467, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
14. A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring of said device's power consumption, comprising: (a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message; (b) an oscillator generating a first clock signal; (c) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; (d) a source of unpredictable information; (e) a clock decorrelator coupled to said source of unpredictable information for	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997)

generating a second clock signal from said first clock signal using said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal; and (f) a processor: (i) clocked by said second clock signal, (ii) configured to cryptographically processing said data, and (iii) configured to output said cryptographically processed data using said input/output interface.	Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.
15. A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:

of said device's power consumption, comprising: (a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message; (b) an input interface for receiving an external clock signal; (c) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; (d) a source of unpredictable information; (e) a clock decorrelator coupled to said source of unpredictable information for generating an internal clock signal from said external clock signal using said unpredictable information, such that said internal clock signal cannot be reliably predicted from said external clock signal; and (f) a processor: (i) clocked by said internal clock signal, (ii) configured to cryptographically processing said data, and (iii) configured to output said cryptographically processed data using said input/output interface.	Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that

	each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.
16. The device of claim 15 wherein said clock decorrelator comprises a clock skipping module which selects a subset of the cycles of said external clock signal to use as said internal clock signal based on said unpredictable information.	**OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the

	references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. The motivation to use an external signal to generate an internal signal may be found, for example, in Sprunk '402 at, *e.g.*, 1:52-54 (random signal to generate clock eliminates the ability to predict the clock even if observable) and/or Sci.crypt Postings at, e.g. posting by Jim Bell, December 24, 1995 (using pseudorandomly varied oscillator would make resulting computer harder to bug). Further, Rankl (1997) at 44 and 264 teaches that smart card processors require an external clock signal.
17. The device of claim 15 wherein said source of unpredictable information comprises a hardware random number generator.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833

	Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either

	explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in combination with one or more of the above listed references, renders the claim invalid as obvious.
18. The device of claim 15 further comprising a monitor for detecting a clock fault in said external clock signal and preventing said processor from processing said quantity if said clock fault is detected.	**OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Griffin '294 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a

	person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. The motivation to a fault monitor as claimed is found, for example, in Griffin '294 at 2:30-36 and generally at 3:37-5:26.
19. The device of claim 15 wherein said clock decorrelator is selectively operable under the control of said processor.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the

	references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in combination with one or more of the above listed references, renders the claim invalid as obvious.
20. The device of claim 15 wherein said clock decorrelator is selectively operable such that said clock decorrelator is disabled when data is being transferred across said input/output interface and enabled during said cryptographic processing operation.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917

	individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Lindholm '725 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in

	combination with one or more of the above listed references, renders the claim invalid as obvious.
21. The device of claim 15 further comprising a noise production system connected to said processor for introducing noise into said measurement of the power consumption by consuming a random amount of power during said cryptographic prosing operation.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective

	functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833, alone or in combination with one or more of the above listed references, renders the claim invalid as obvious.
22. A device according to claims 1, 4, 7, 9, 11, 14, 15, or 20 wherein said device comprises a smartcard.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Sci.crypt Postings Dunlavy '201 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the above listed references, individually or in combination with one or more of the following references: Ugon '833 Griffin '294

	Sci.crypt Postings Dunlavy '201 Hoppe '894 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) ISO 7816 Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. Each of Ugon '833, Griffin '294, the Sci.crypt Postings, and Dunlavy '201 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
23. A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following

within a cryptographic processing device by external monitoring, comprising: (a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) generating unpredictable information; (c) cryptographically processing said quantity, including using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting between: (c)(1) performing a computation and incorporating the result of said computation in said cryptographic processing, and (c)(2) performing a computation whose output is not incorporated in said cryptographic processing; and (d) outputting said cryptographically processed quantity to a recipient thereof.	reference: Dunlavy '201 The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious by any of the references or combinations of references showing obviousness of claim 1. Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed components had been or could be used with cryptographic processing devices; and/or (6) a suggestion in the reference that the disclosed components had been or could be used with cryptographic processing devices. For example, ISO 7816 shows standard pin assignments, which include

	an I/O interface. Each of Ugon '833 and Dunlavy '201 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, either of these references renders the claim obvious, alone or in combination with any of the above listed references.
24. The method of claim 23 where said selecting is performed in software.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117 individually or in combination with one or more of the following references: Ugon '833 Griffin '294 Sci.crypt Postings Malek '467

	Van Eck '117 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Each of Ugon '833, Griffin '294, the Sci.crypt Postings, Malek '467 and Van Eck '117 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
25. The method of claim 23 where said selecting is performed in hardware on an integrated circuit including a	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references:

microprocessor.	Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117 individually or in combination with one or more of the following references: Ugon '833 Griffin '294 Sci.crypt Postings Malek '467 Van Eck '117 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify.

	SUGGESTION OR MOTIVATION TO COMBINE Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Each of Ugon '833, Griffin '294, the Sci.crypt Postings, Malek '467 and Van Eck '117 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
26. A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising: (a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) generating unpredictable information; (c) cryptographically processing said quantity, including using said unpredictable	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Van Eck '117 Hoivik '098 The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference: Ugon '833 **OBVIOUSNESS**

information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by selecting a code process from a plurality of code processes, where said selected code process is involved in said cryptographic processing, but where the value of said outputted quantity is independent of which of said code processes was selected; and (d) outputting said cryptographically processed quantity to a recipient thereof.	The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Griffin '294 Van Eck '117 Hoivik '098 individually or in combination with one or more of the following references: Ugon '833 Griffin '294 Van Eck '117 Hoivik '098 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that

	each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Griffin '294, Van Eck '117, and Hoivik '098 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
27. A method of securely performing a cryptographic processing operation including a sequence of instructions in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising: (a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) generating unpredictable information; (c) using said unpredictable information while processing said quantity to conceal a	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Dunlavy '201 Lindholm '713 Sci.crypt Postings The claim is anticipated under 35 U.S.C. § 102 (e) by the following reference: Ugon '833 **OBVIOUSNESS**

correlation between externally monitorable signals and said secret by using said unpredictable information to modify said sequence; and (d) outputting said cryptographically processed quantity to a recipient thereof.	The claim is rendered obvious under 35 U.S.C. §103 by the following references: Griffin '294 Dunlavy '201 Lindholm '713 Sci.crypt Postings Ugon '833 individually or in combination with one or more of the following references: Griffin '294 Dunlavy '201 Lindholm '713 Sci.crypt Postings Ugon '833 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person

	of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Griffin '294, Lindholm '713, Dunlavy '201, and the Sci.crypt Postings fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
28. A method of securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising: (a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (b) generating unpredictable information; (c) using said unpredictable information	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Sci.crypt Postings Lindholm '725 Van Eck '117 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by one or more of the following references: Sci.crypt Postings

while processing said quantity to conceal a correlation between externally monitorable signals and said secret by randomizing the order of said permutation; and (d) outputting said cryptographically processed quantity to a recipient thereof.	Ugon '833 Lindholm '725 Van Eck '117 Dunlavy '201 individually or in combination with one or more of the following references: Sci.crypt Postings Ugon '833 Lindholm '725 Van Eck '117 Dunlavy '201 Hoppe '894 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) ISO 7816 FIPS Pub 46-2 (1993) Menezes (1997) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that

	each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. For example, Menezes (1997) at 10 teaches that permutations are commonly used in cryptographic operations. Each of Van Eck '117, Lindholm '725, and the Sci.crypt Postings fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
29. A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising: (a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; (b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; (c) introducing noise into said measurement of said power consumption while processing said quantity; and (d) outputting said cryptographically processed quantity to a recipient thereof.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Sci.crypt Postings Fruhauf '053 Sprunk '402 Lisimaque '039 Kolbert '057 Lindholm '725 Meyr '962 Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references:

	Ugon '833 Wuidart '917 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Griffin '294 Sci.crypt Postings Fruhauf '053 Sprunk '402 Lisimaque '039 Kolbert '057 Lindholm '725 Meyr '962 Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Griffin '294 Sci.crypt Postings Fruhauf '053 Sprunk '402 Lisimaque '039 Kolbert '057

	Lindholm '725 Meyr '962 Nossen '423 Lindholm '713 Saltwick '243 Malek '467 Van Eck '117 Dunlavy '201 Høivik '098 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods.

	Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, each of Griffin '294, the Sci.crypt Postings, Fruhauf '053, Sprunk '402, Lisimaque '039, Kolbert '057, Lindholm '725, Meyr '962, Nossen '423, Lindholm '713, Saltwick '243, Malek '467, Van Eck '117, Dunlavy '201, Høivik '098, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
30. The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic; (b) improving the random characteristic of said initial noise; and (c) varying said power consumption based on said improved initial noise.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (a) and/or (b) by the following references: Griffin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098 The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 Wuidart '917

	OBVIOUSNESS The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 Griffin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Griffin '294 Fruhauf '053 Lindholm '725 Lindholm '713 Saltwick '243 Malek '467 Høivik '098 Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE**

	Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Each of Ugon '833, Griffin '294, Fruhauf '053, Lindholm '725, Lindholm '713, Saltwick '243, Malek '467, Høivik '098, and Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, any of these references renders the claim obvious, alone or in combination with any of the above listed references.
31. A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising: (a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; (b) generating a first clock signal; (c) receiving data to be cryptographically	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 Wuidart '917 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917

processed, said data being representative of at least a portion of a message; (d) generating unpredictable information; (e) generating a second clock signal from said first clock signal using said unpredictable information, such that said second clock signal cannot be reliably predicted from said first clock signal; (f) processing said data using said second clock signal; and (g) outputting said cryptographically processed quantity to a recipient thereof.	individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example,

	Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious. Similarly, Wuidart '917 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Wuidart '917 renders the claim obvious, alone or in combination with any of the above listed references.
32. A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising: (a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; (b) receiving an external clock signal; (c) receiving data to be cryptographically processed, said data being representative of at least a portion of a message; (d) generating unpredictable information; (e) generating an internal clock signal from said external clock signal using said unpredictable information, such that said external clock signal cannot be reliably predicted from said internal clock signal; (f) processing said data using said internal	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987)

clock signal; and (g) outputting said cryptographically processed quantity to a recipient thereof.	Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the event that Ugon '833 does not fully anticipate the claim, it nevertheless renders the claim invalid as obvious. For example, Ugon '833 teaches all elements of the claim and provides motivation to combine them, *e.g.*, at 3:59-4:8 (the disclosed improvements are designed for use in ST16XY cards); 1:14-19 (the disclosed improvements are intended to be implemented in microprocessors and microcomputers which require protection). In the alternative, Ugon '833, in combination with one or more of the above listed references, renders the claim invalid as obvious.
33. The method of claim 32 wherein said step of generating said internal clock signal comprises a step of selecting a subset of the cycles of said external clock signal to use as said internal clock signal based on said	**OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917

unpredictable information.	individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. The motivation to use an external signal to generate an internal signal based on unpredictable information may be found, for example, in Sprunk '402 at, *e.g.*, 1:52-54 (random signal to generate clock eliminates the ability to predict the clock even if

	observable), and/or Sci.crypt Postings at, e.g. posting by Jim Bell, December 24, 1995 (using pseudorandomly varied oscillator would make resulting computer harder to bug).
34. The method of claim 32 wherein said step of generating unpredictable information comprises a step of generating a random number.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida

	v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833 renders the claim obvious, alone or in combination with any of the above listed references.
35. The method of claim 32 further comprising a step of monitoring for a clock fault in said external clock signal and a step of preventing said processor from outputting said cryptographically processed quantity if said clock fault is detected.	**OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833 Wuidart '917 Sprunk '402 Griffin '294 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the

	references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. The motivation to implement a fault monitor as claimed is found, for example, in Griffin '294 at 2:30-36 and generally at 3:37-5:26.
36. The method of claim 32 further comprising a step of introducing noise into said measurement of the power consumption.	**ANTICIPATION** The claim is anticipated under 35 U.S.C. § 102 (e) by the following references: Ugon '833 **OBVIOUSNESS** The claim is rendered obvious under 35 U.S.C. §103 by the following references: Ugon '833 Wuidart '917 individually or in combination with one or more of the following references: Ugon '833

	Wuidart '917 Sprunk '402 Sci.crypt Postings Hoppe '894 ISO 7816 Wakerly (1989) Rankl (1997) Schaumüller-Bichl (1987) Further, Visa reserves the right to demonstrate invalidity using one or more of the references listed in Exhibit A-1, and any other art it may later identify. **SUGGESTION OR MOTIVATION TO COMBINE** Initially, no suggestion or motivation to combine one or more of the references listed above is required to render the claim obvious under 35 U.S.C. § 103 as the claim merely sets forth a combination of existing elements with no change in their respective functions nor does the combination provide a new or different function. See Sakraida v. Ag Pro, Inc., 425 U.S. 273, 282 (1976); Anderson's-Black Rock, Inc. v. Pavement Salvage Co., 396 U.S. 57, 60 (1969). Notwithstanding the foregoing, an explicit and/or implicit teaching, suggestion, or inference to combine one or more of the references listed above is provided by: (1) the knowledge generally available to a person of ordinary skill in the art; (2) the prior art references as understood by a person of ordinary skill in the art; (3) the nature of the problem to be solved; (4) the fact that each prior art reference involves similar problems; (5) the knowledge of those skilled in the art that the disclosed methods had been or could be used with cryptographic processing methods; and/or (6) a suggestion in the reference that the disclosed methods had been or could be used with cryptographic processing methods. Ugon '833 fully anticipates the claim by disclosing each of the claimed elements either explicitly, implicitly, or inherently. In the alternative, Ugon '833 renders the claim obvious, alone or in combination with any of the above listed references.